CERT

Insider Threats:

Challenges with Trusted Business Partners

12 September 2011

Randall Trzeciak

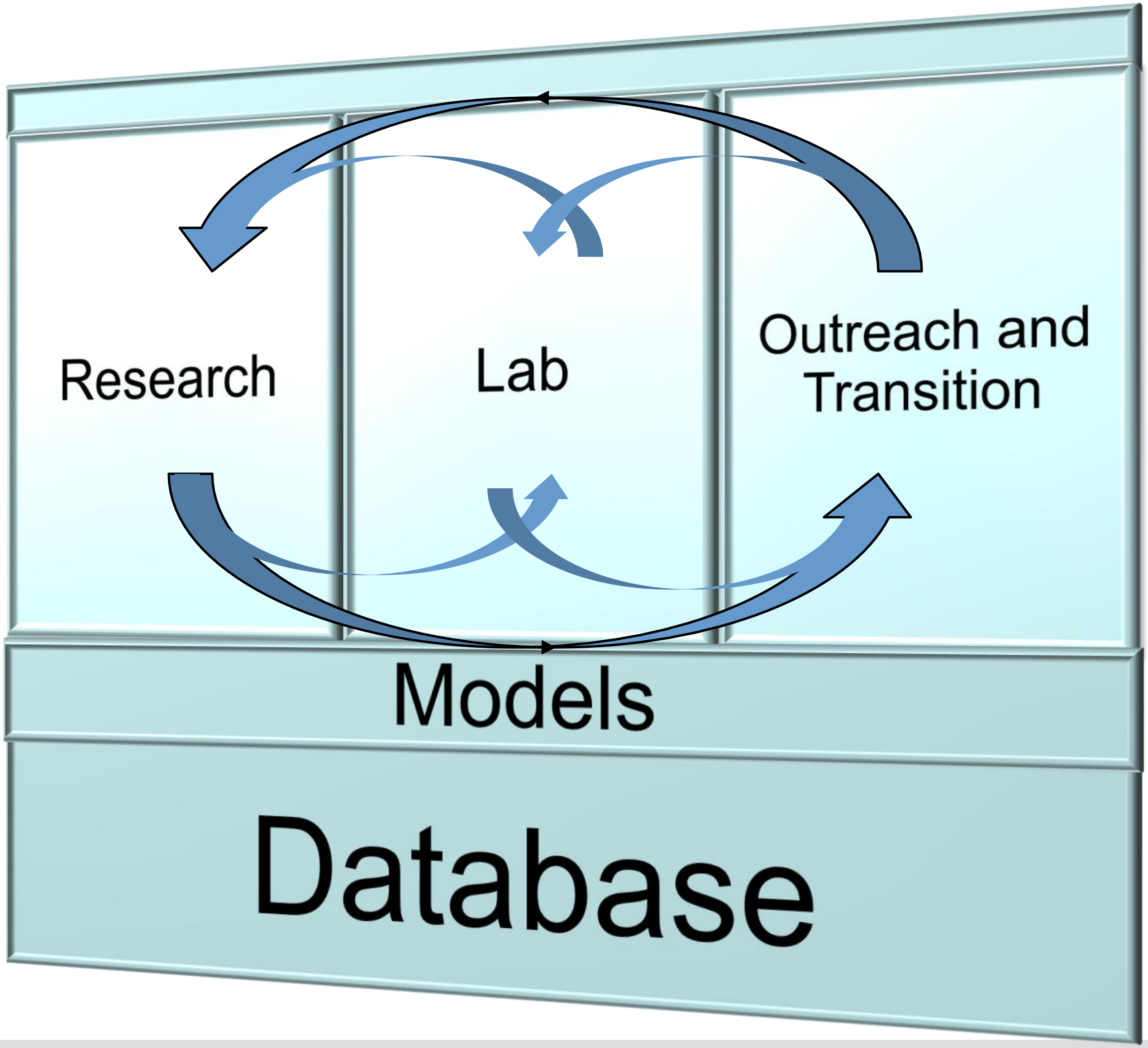
© 2007-2011 Carnegie Mellon University

Who is a Malicious Insider?

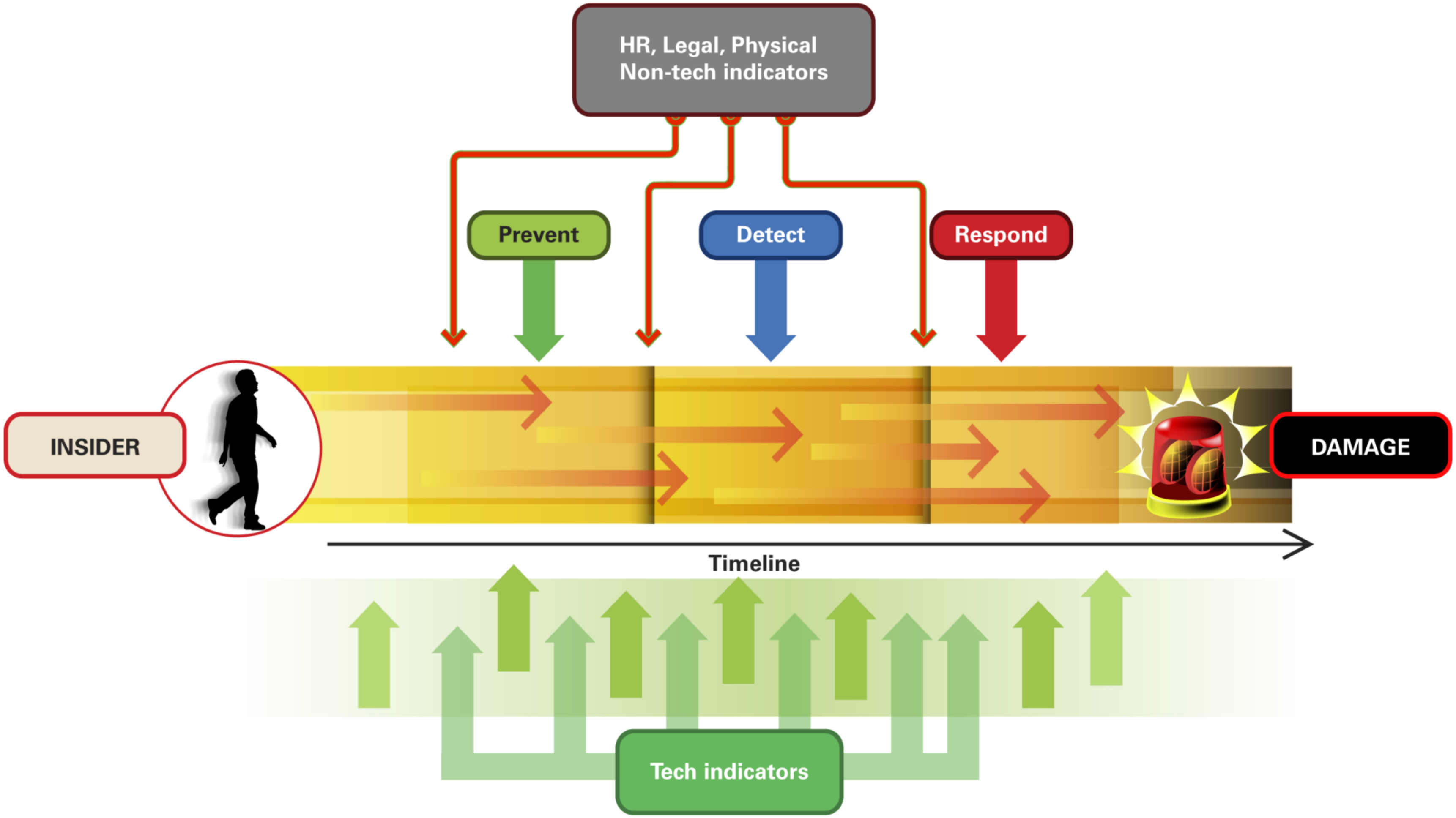
Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization’s network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.*

CERT’s Unique Approach to the Problem

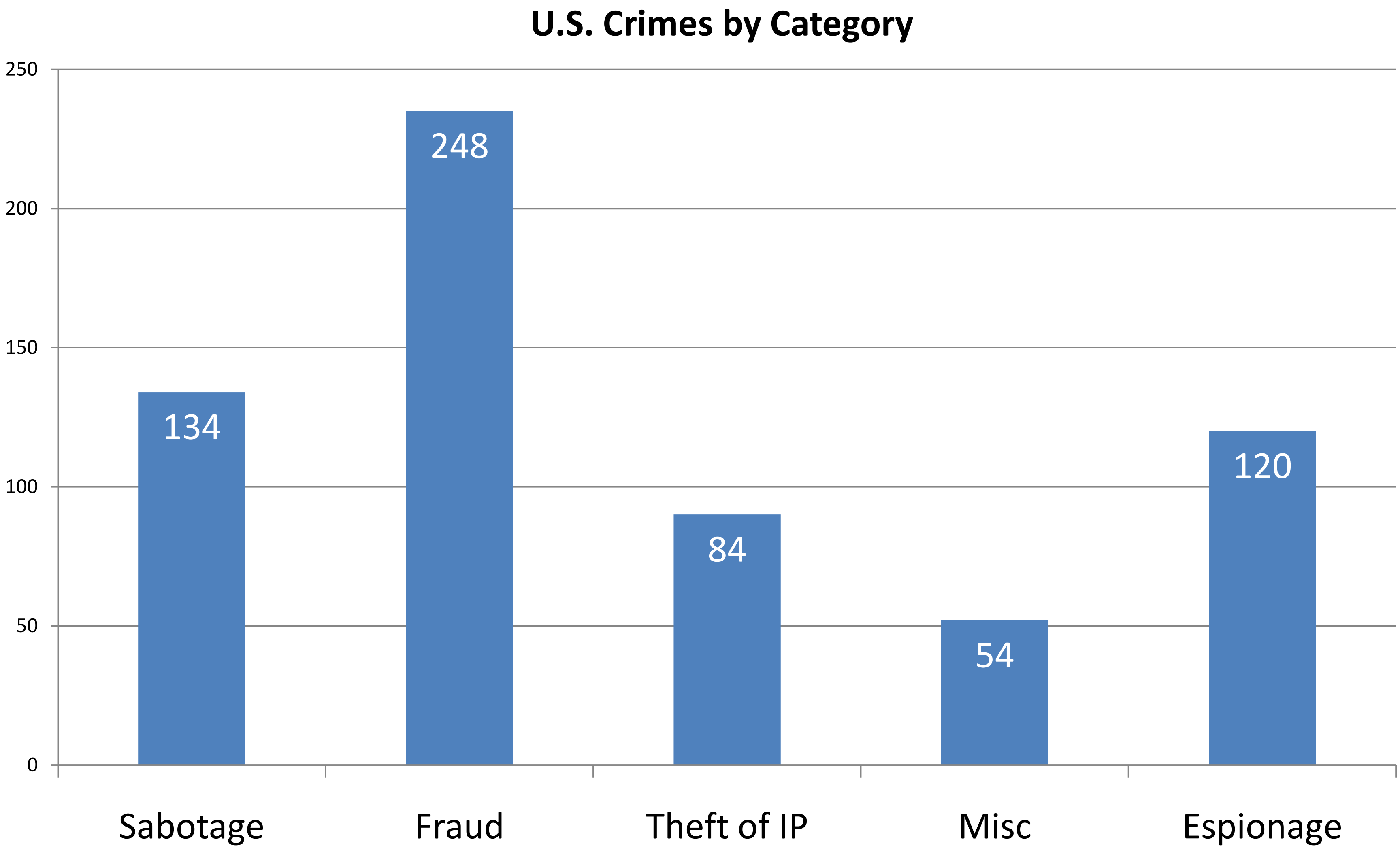


CERT Insider Threat Center Objective

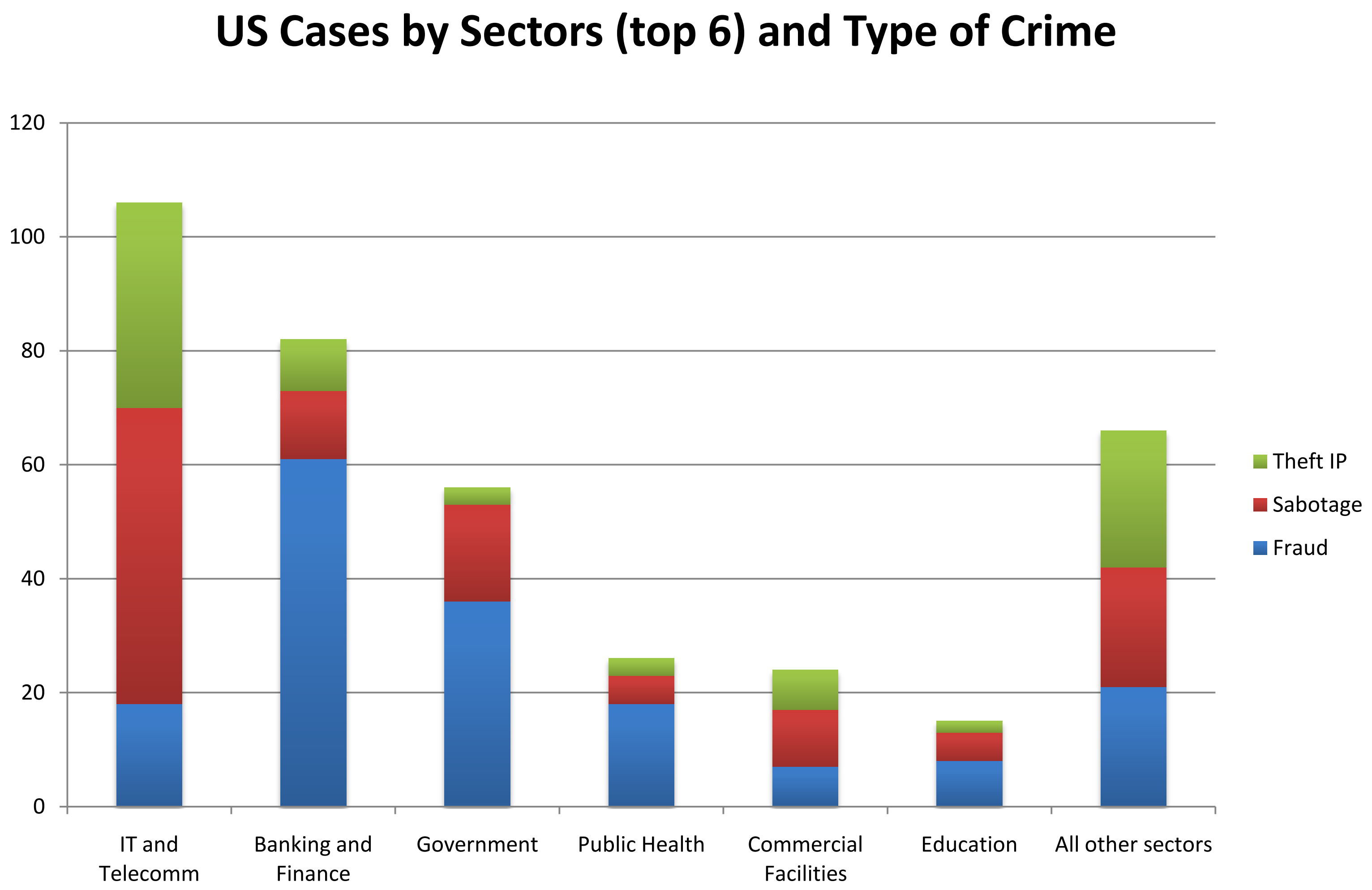


Opportunities for prevention, detection, and response for an insider attack

CERT’s Insider Threat Case Database



Critical Infrastructure Sectors



How bad is the insider threat?

Insider Threat Issue

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers’ systems and/or databases.

Insiders can bypass existing physical and electronic security measures through ***legitimate*** measures.

2011 CyberSecurity Watch Survey -1

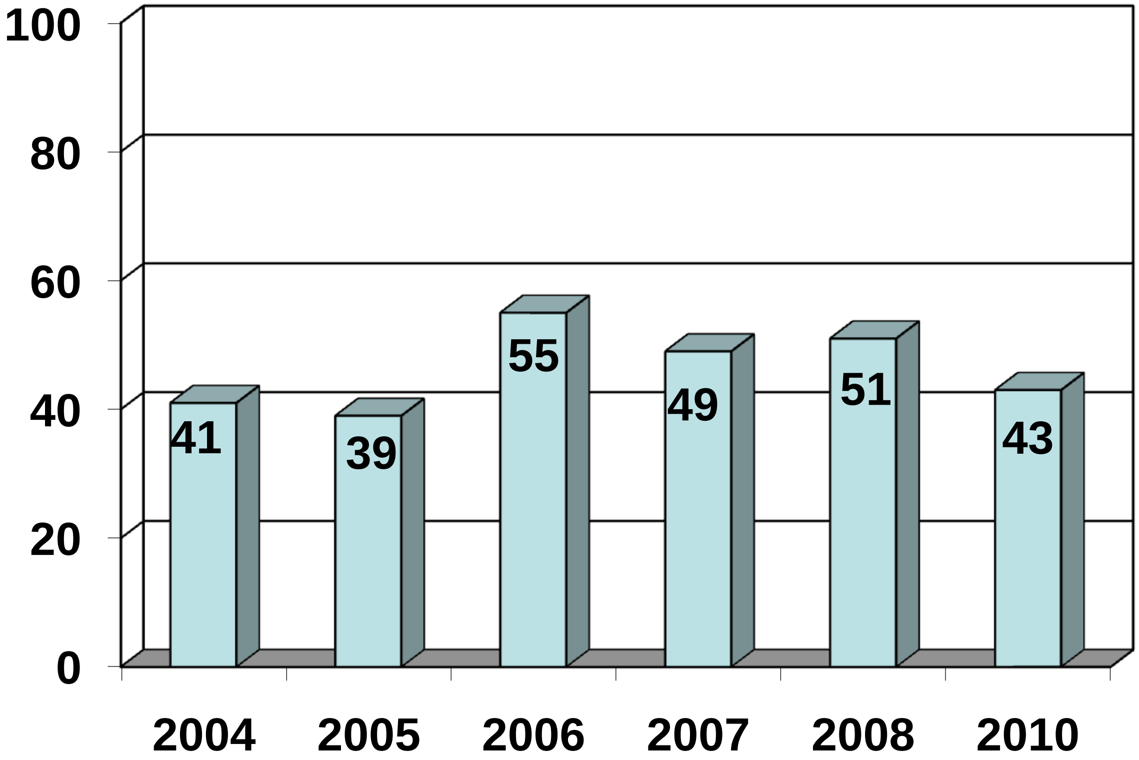
CSO Magazine, USSS, CERT & Deloitte

607 respondents

38% of organizations have more than 5000 employees

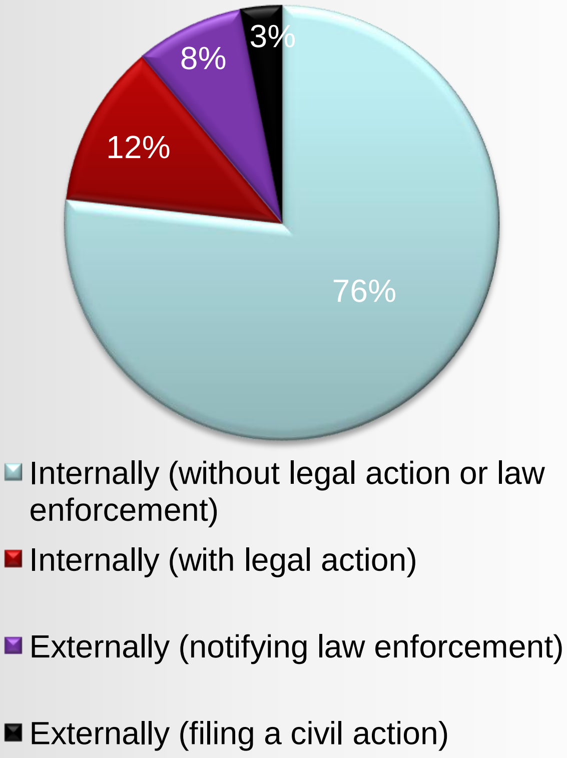
37% of organizations have less than 500 employees

Percentage of Participants Who Experienced an Insider Incident



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurity Watch Survey - 2


How Insider Intrusions Are Handled

Reason(s) CyberCrimes were not referred for legal action

	2011	2010
Damage level insufficient to warrant prosecution	42%	37%
Could not identify the individual/ individuals responsible for committing the eCrime	40%	29%
Lack of evidence/not enough information to prosecute	39%	35%
Concerns about negative publicity	12%	15%
Concerns about liability	8%	7%
Concerns that competitors would use incident to their advantage	6%	5%
Prior negative response from law enforcement	5%	7%
Unaware that we could report these crimes	4%	5%
Other	11%	5%
Don't know	20%	14%
Not applicable	N/A	24%

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

Insider Threat: Trusted Business Partners

Insider Threat: Trusted Business Partners

Spotlight On: Insider Threat from Trusted Business Partners

February 2010

Robert M. Weiland
Andrew P. Moore
Dawn M. Cappelli
Randall F. Trzeciak
Derrick Spooner

This work was funded by
CyLab
www.cylab.cmu.edu

What is a Trusted Business Partner

Any external organization or individual an organization has contracted to perform a service.

- Authorized access to proprietary data, critical files, and/or internal infrastructure
- Organizational Relationship: one organization outsources a service to a TBP
- Individual Relationship: consultants, temporary employees, and contracted employees

IT Sabotage

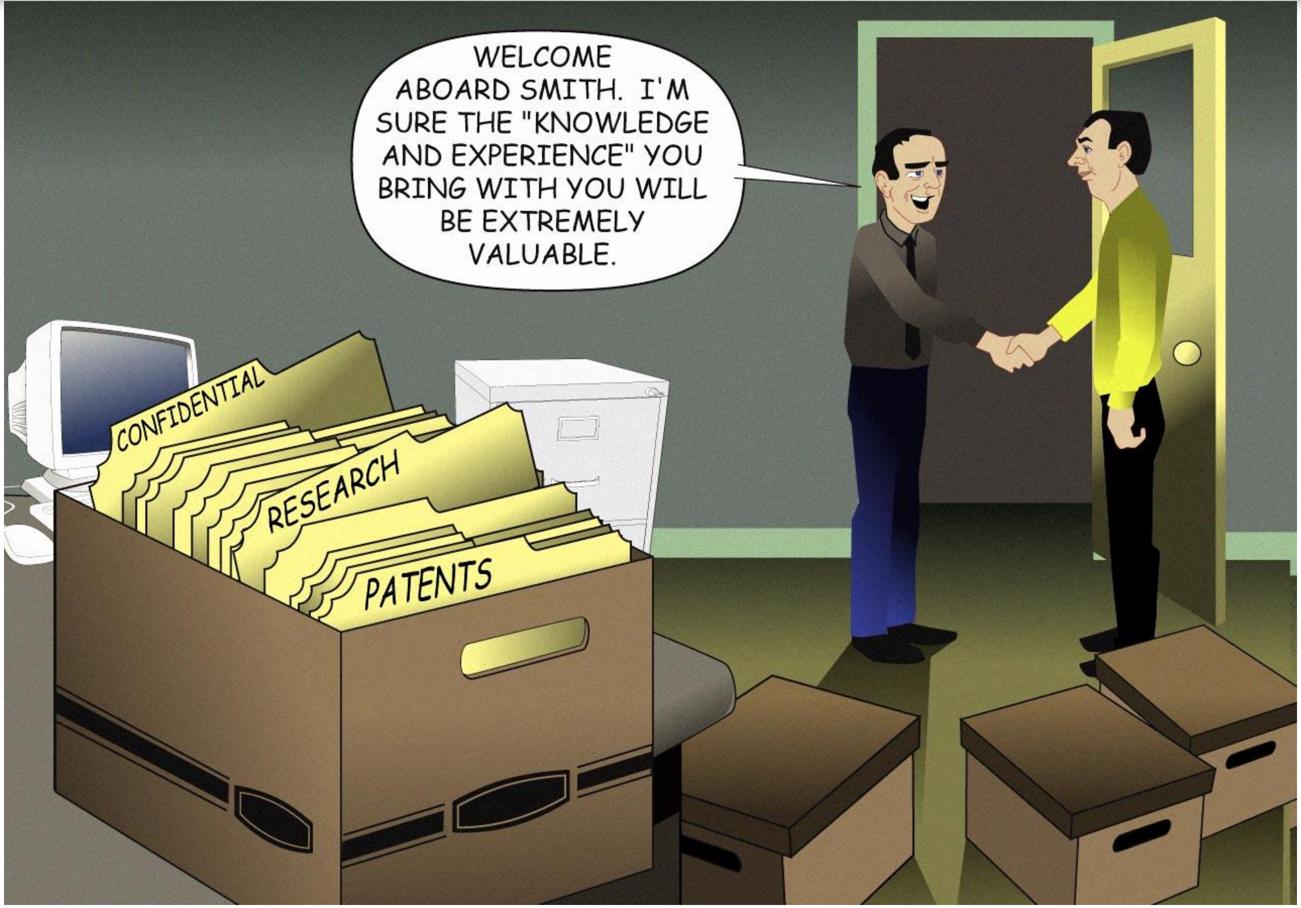
DAN
DAN
SLAM!
Attach File(s)
Do you want to attach DAN_BACKDOOR.EXE?
YES
NO

TRUE STORY:

A company’s mobile devices were suddenly disabled for almost 1000 employees, grinding sales and delivery operations to a halt for several days …

Logic bomb goes off three months to the day after a demoted system architect’s retaliatory resignation.

Theft of Intellectual Property


WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
CONFIDENTIAL
RESEARCH
PATENTS

TRUE STORY:

A new employee at a networking firm starts developing a competitive product based on the victim firm's source code after less than a month on the job.

The insider was confronted by his former employer and investigators found copies of their source code on his home computer.

Fraud

TRUE STORY:

An insider at a financial organization modifies critical source code to syphon off money to cover fraudulent personal loans he had created.

The insider had stolen over $90,000 before finally being caught on a routine audit of loans with abnormal terms.

Insider Threats During the SDLC

Phases of the Life Cycle Exploited

Requirements definition

System design

System implementation

System deployment

System maintenance

Requirements Definition Oversights

Neglecting to define **authentication** and **role-based access control** requirements simplified insider attacks.

Neglecting to define **security requirements/separation of duties** for **automated business processes** provided an easy method for insider attack.

Neglecting to define requirements for **automated data integrity checks** gave insiders the security of knowing their actions would not be detected.

System Design Oversights

Insufficient attention to security details in **automated workflow processes** enabled insiders to commit malicious activity.

Insufficient **separation of duties** facilitated insider crimes.

- not designed at all
- no one to “check the checker”

Neglecting to consider security vulnerabilities posed by “**authorized system overrides**” resulted in an easy method for insiders to ”get around the rules”.

System Implementation Exploits

Lack of **code reviews** allowed insertion of “backdoors” into source code.

Inability to **attribute actions** to a single user enabled a project leader to sabotage his own team’s development project.

System Deployment Oversights

Lack of enforcement of **documentation practices** and **backup procedures** prohibited recovery efforts when an insider deleted the only copy of source code for a production system.

Use of the same **password file** for development and the operational system enabled insiders to access and steal sensitive data from the operational system.

Unrestricted access to all customers' systems enabled a computer technician to plant a virus directly on customer networks.

Lack of **configuration control** and well-defined **business processes** enabled libelous material to be published to organization's website.

System Maintenance Issues

Lack of **code reviews** facilitated insertion of malicious code.

Ineffective **configuration control** practices enabled release of unauthorized code into production.

Ineffective or lack of **backup processes** amplified the impact of mass deletion of data.

End-user access to source code for systems they used enabled modification of security measures built into the source code.

Ignoring known **system vulnerabilities** provided an easy exploit method.

Common Sense Guide to Prevention and Detection of Insider Threats

http://www.cert.org/archive/pdf/CSG-V3.pdf

TBP Recommendations for Mitigation and Detection

Understand the policies and procedures of the trusted business partner.

Monitor intellectual property to which access is provided.

Maintain access rights management.

Understand the personnel policies and procedures of the trusted business partner.

Anticipate and manage negative workplace issues.

Deactivate access following termination.

Enforce separation of duties.

Create clear contractual agreements that make it clear the TBP is also responsible for protecting organizational resources.

Summary of Best Practices in CSG

Consider threats from insiders and business partners in enterprise-wide risk assessments.

Clearly document and consistently enforce policies and controls.

Institute periodic security awareness training for all employees.

Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.

Anticipate and manage negative workplace issues.

Track and secure the physical environment.

Implement strict password and account management policies and practices.

Enforce separation of duties and least privilege.

Consider insider threats in the software development life cycle.

Use extra caution with system administrators and technical or privileged users.

Implement system change controls.

Log, monitor, and audit employee online actions.

Use layered defense against remote attacks.

Deactivate computer access following termination.

Implement secure backup and recovery processes.

Develop an insider incident response plan.

Points of Contact

Insider Threat Center
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

Randall Trzeciak
Technical Team Lead
+1 412 268-7040
rft@cert.org

http://www.cert.org/insider_threat/